JOURNAL
de Théorie des Nombres
de BORDEAUX
*anciennement Séminaire de Théorie des Nombres de Bordeaux*

Franck LALANDE

**A propos de la relation galoisienne $x_1 = x_2 + x_3$**

Tome 22, n° 3 (2010), p. 661-673.

<http://jtnb.cedram.org/item?id=JTNB_2010__22_3_661_0>

*Journal de Théorie des Nombres*
*de Bordeaux* **22** (2010), 661-673

# A propos de la relation galoisienne $x_1 = x_2 + x_3$

par Franck LALANDE

Résumé. L'existence d'un polynôme $f$, irréductible sur un corps $k$ de caractéristique 0 et dont trois racines vérifient la relation linéaire $x_1 = x_2 + x_3$, ne dépend que de la paire de groupes finis $(G, H)$ où $G = \mathrm{Gal}_k(f)$ et $H \subset G$ est le fixateur d'une racine. Le cas régulier ($H = 1$) est désormais assez bien décrit. On démontre dans ce texte que pour de nombreuses paires $(G, H)$ primitives ($H$ sous-groupe maximal de $G$) et en particulier pour toutes celles de degré $\leq 50$, la relation $x_1 = x_2 + x_3$ n'est pas réalisable.

En appendice, Joseph Oesterlé démontre que cette relation linéaire est réalisable pour la paire $(G, 1)$ dès que 6 divise l'ordre de $G$.

Abstract. *About the Galois relation* $x_1 = x_2 + x_3$

Let $k$ be a field of characteristic 0. The existence of an irreducible polynomial $f$ over $k$ whose roots satisfy the linear relation $x_1 = x_2 + x_3$ exclusively depends on the pair $(G, H)$ where $G = \mathrm{Gal}_k(f)$ and $H \subset G$ is the stabilizer of one root. The regular case ($H = 1$) is now well understood. In the present paper, we consider the primitive case ($H$ maximal subgroup of $G$) and show that we can't find this linear relation when the pair $(G, H)$ is primitive of a degree $\leq 50$.

An appendix of Joseph Oesterlé shows that we can find this relation for any pair $(G, 1)$ in which 6 divides the order of $G$.

## 1. Introduction

Soient $k$ un corps de caractéristique 0, $G$ un groupe fini réalisable comme groupe de Galois sur $k$ et $H$ un sous-groupe de $G$. Soit $e_H = \frac{1}{|H|} \sum_{h \in H} h$. C'est un élément idempotent de $k[G]$ et le sous-$k[G]$-module $k[G]e_H$ de $k[G]$ est isomorphe au $k[G]$-module $k[G/H]$. Il est induit par le $k[H]$-module $ke_H$, on notera $1_H^G$ son caractère dans la suite. Un élément $a$ de $k[G]e_H$ est dit *admissible* si le sous-module $k[G]a$ ne contient aucun élément non nul de la forme $(g-1)e_H$. Diverses caractérisations des éléments admissibles sont utilisées et bien connues, elles sont dues à Kurt Girstmair (voir [4]).

Manuscrit reçu le 25 juin 2009.

**Proposition 1.** *i) Pour qu'un élément $a$ de $k[G]e_H$ soit admissible, il faut et il suffit qu'il existe $\beta \in k[G]$ tel que $a\beta = 0$ et dont le fixateur $G_\beta$ sous l'action à gauche de $G$ soit exactement $H$ .*
*ii) Soit $L$ une extension galoisienne de $k$ de groupe de Galois $G$. Pour que $a \in k[G]e_H$ soit admissible, il faut et il suffit qu'il existe un élément primitif $x$ du sous-corps $L^H$ de $L$ fixé par $H$ tel que $ax = 0$ .*

D'après ii), rechercher un polynôme irréductible $f$ de $k[X]$ et de groupe de Galois $G$, dont certaines racines vérifient la relation linéaire $x_1 = x_2 + x_3$ revient donc à chercher un élément admissible de $k[G]e_H$ de la forme $a = (1 - s - t)e_H$ où $H$ est le fixateur d'une racine de $f$ et où $s$ et $t$ sont deux éléments de $G$ distincts et distincts de 1 modulo $H$.

**Remarque.** Le rôle de $H$ est essentiel. On sait par exemple qu'il n'existe aucun élément admissible dans $k[G]e_H$ différent de $e_G = \frac{1}{|G|}\sum_{g\in G} g$ lorsque la représentation de permutation

$$G \longrightarrow Perm(G/H) \ : \ g \longmapsto \rho_g : \ (sH) \longmapsto (gsH)$$

est 2-transitive alors qu'il est souvent aisé de déterminer des éléments admissibles lorsque $H = 1$. Nous supposerons toujours dans la suite cette représentation *fidèle*. Cela signifie que le sous-groupe $F = \cap_g \, gHg^{-1}$ est réduit à 1 ou autrement dit que $L$ est la clôtute galoisienne de $L^H$. Cette représentation est dite *régulière* lorsque $H = 1$ et *primitive* lorsque $H$ est un sous-groupe maximal de $G$.

Le cas régulier est le mieux connu actuellement. Si $G$ est abelien, des théorèmes de [1] et [4] affirment que pour qu'il existe un élément admissible dans $k[G]$ de la forme $a = 1 - s - t$, il faut et il suffit que l'ordre de $G$ soit un multiple de 6. D'après [5] et [8], il existe un élément $a = 1 - s - t$ admissible dans $k[G]$ dès que $G$ contient un sous-groupe d'ordre 6 et il a été demandé à plusieurs reprises si une condition suffisante pour l'existence dans $k[G]$ d'un tel élément admissible n'est pas seulement que l'ordre de $G$ soit un multiple de 6. La réponse est positive comme l'assure le théorème de Joseph Oesterlé qui suit et dont la démonstration est donnée en appendice.

**Théorème 1** (J. Oesterlé)**.** *Supposons que l'ordre de $G$ soit multiple de 6. Soient $s$ un élément de $G$ d'ordre 2 et $t$ un élément de $G$ d'ordre 3. Alors $a = 1 - st - st^2$ est un élément admissible de $k[G]$ .*

Cette condition sur l'ordre de $G$ n'est pas nécessaire. Voir pour cela [5] .

On se place dans la suite dans le cas non régulier ($H \neq 1$), ce qui revient rappelons-le à abaisser le degré du polynôme $f$ de groupe $G$. Ce degré est en quelque sorte minimal lorsque la paire $(G, H)$ est primitive. C'est la situation dans laquelle on se place aux paragraphes 3 et 4 et nous démontrons que pour de nombreuses paires primitives (et en particulier toutes celles

de degré $\leq 50$), il est impossible d'obtenir la relation $x_1 = x_2 + x_3$. Signalons enfin qu'aucune relation de longueur 3 exceptée la relation triviale $x_1 + x_2 + x_3 = 0$ en degré 3 n'est actuellement connue dans le cas primitif.

## 2. Quelques remarques à propos des paires non régulières

Dans toute la suite, $H$ désigne un sous-groupe de $G$ (il sera supposé maximal dans les sections suivantes). Le groupe $H$ agit par multiplication à gauche sur les classes à gauche $sH$ de $G$ modulo $H$. Pour $s \in G$, nous dirons que l'orbite $H\overline{s}$ de la classe $\overline{s} = sH$ est *réflexive* (*self-paired* en anglais) si elle contient la classe $s^{-1}H$. Le nombre d'orbites s'appelle le *rang* de la paire $(G, H)$, leurs longueurs $n_1 = 1, n_2, \ldots, n_r$ sont appelées les *sous-degrés*. Un rang égal à 2 signifie que l'action de $G$ sur les $sH$ est 2-transitive. Pour un élément $x = \sum a_g g$ de $k[G]$, on définit le *poids* de $x$ comme étant $p(x) = \sum a_g$. C'est un morphisme d'algèbres de $k[G]$ dans $k$.

Commençons par quelques exemples. La proposition qui suit est basée sur une idée de Dubickas (voir [5] ).

**Proposition 2.** *Soit $G$ un groupe fini qui possède une représentation 2-transitive et fidèle en degré $d$. Il existe un sous-groupe $H$ de $G$ d'indice $d(d-1)$ et deux éléments $s$ et $t$ distincts et distincts de 1 modulo $H$ tels que $a = (1 - s - t)e_H$ soit admissible dans $k[G]e_H$.*

Soit $H'$ un sous-groupe de $G$ pour lequel l'action de $G$ sur les classes à gauche $gH'$ de $G$ modulo $H'$ est 2-transitive et fidèle. Soit $L$ une extension galoisienne de $k$ de groupe $G$ et soit $x$ un élément primitif du corps $L^{H'}$. On note $x_j$ ses conjugués et on pose $y = x_1 - x_2$. Si $x$ est de degré $d$, $y$ est de degré $d(d-1)$ car par hypothèse, tous les $y_{i,j} = x_i - x_j$ sont des conjugués de $y$ et sont de plus tous distincts car sinon les conjugués de $x$ vérifieraient une relation du type $x_1 - x_2 = x_i - x_j$, ce qui est contradictoire avec le fait que la paire $(G, H')$ soit 2-transitive. En effet, d'après [4], si la paire $(G, H')$ est 2-transitive, $e_G$ est le seul élément admissible de $k[G]e_{H'}$, autrement dit, seule la relation triviale $\sum x_i = 0$ est possible.

Les conjugués de $y$ vérifient la relation $y_{1,3} = y_{1,2} + y_{2,3}$ et engendrent le corps $L$ car si un élément de $G$ fixe tous les $y_{i,j}$, il fixe tous les $x_i$. Si on note $H$ le fixateur de $y$, il existe un élément $a = (1 - s - t)e_H$ admissible de $k[G]e_H$.

**Exemple.** Pour tout entier $d \geq 3$, la paire $(S_d, S_{d-1})$ est 2-transitive. La propriété ci-dessus assure alors l'existence d'un élément admissible de la forme $(1 - s - t)e_H$ pour la paire $(G, H) = (S_d, S_{d-2})$. Autrement dit, pour toute extension galoisienne $L/k$ de groupe de Galois $S_d$, il existe un polynôme $f$ de $k[X]$ irréductible de degré $d(d-1)$, de corps de décomposition $L$ et dont trois racines vérifient la relation $x_1 = x_2 + x_3$.

Lorsque les sous-degrés sont distincts, on ne peut obtenir que très peu de relations de longueur 3. C'est l'objet des deux propositions qui suivent.

**Proposition 3.** *Si les sous-degrés sont distincts, aucun élément de la forme* $a = (1-s-t)e_H$ *avec* $1 \neq s \neq t \neq 1$ $(mod\ H)$ *n'est admissible dans* $k[G]e_H$.

Soit donc un élément $a = (1-s-t)e_H$ avec $1 \neq s \neq t \neq 1$ $(mod\ H)$. On note $V = k[G]a$ et posons $b = -s^{-1}a = (1-s^{-1}+s^{-1}t)e_H \in V$. De deux choses l'une, les classes $s^{-1}H$ et $s^{-1}tH$ sont ou non dans la même orbite sous l'action de $H$. Si c'est le cas, il existe $h \in H$ tel que $s^{-1}tH = hs^{-1}H$ et $e_H b = e_H(1-s^{-1}+hs^{-1})e_H = e_H \in V$. L'élément $a$ n'est alors pas admissible.

Si ces deux classes sont dans des orbites distintes de longueurs respectives $n_i$ et $n_j$, leurs fixateurs sous l'action de $H$ sont deux sous-groupes de $H$ d'ordres respectifs $|H|/n_i$ et $|H|/n_j$, distincts par hypothèse. Il existe alors un élément $h_0 \in H$ appartenant à un et un seul de ces deux fixateurs et $h_0 b - b$ vaut alors $h_0 b - b = (h_0 s^{-1}t - s^{-1}t)e_H$ ou $h_0 b - b = (s^{-1} - h_0 s^{-1})e_H$. Dans les deux cas, $V$ contient alors un élément non nul du type $(g-1)e_H$ et $a$ n'est pas admissible.

Si le corps de base est le corps $\mathbb{Q}$ des nombres rationnels, la proposition ci-dessus s'étend à toute relation de longueur 3, distincte de $x_1+x_2+x_3 = 0$.

**Proposition 4.** *Si les sous-degrés sont distincts, aucun élément de la forme* $u = (1-\alpha s-\beta t)e_H$ *avec* $1 \neq s \neq t \neq 1$ $(mod\ H)$ *et différent de* $(1+s+t)e_H$ *n'est admissible dans* $\mathbb{Q}[G]e_H$.

Si $\alpha + \beta = \pm 1$, $u$ n'est pas admissible. En effet, à permutation près des trois coefficients $(a_i, a_j, a_k) = (1, -\alpha, -\beta)$, on a $|a_i| = |a_j| + |a_k|$. Dans ce cas, une relation du type $a_i x_i = \pm a_j x_j \pm a_k x_k$ est clairement impossible lorsque les $x_i$ sont des nombres complexes dont on peut considérer le module. La transitivité de $G$ permet en effet de supposer $x_i$ de module maximal et de plus les coefficients de la relation sont réels. D'autre part, si $s$ et $t$ ne sont pas dans la même orbite, ils n'ont pas le même fixateur et on vérifie comme dans la proposition précédente que $V = k[G]u$ contient un élément non nul de la forme $(g-1)e_H$.

On peut donc supposer que $u = (1-\alpha s-\beta h_0 s)e_H$ avec $\alpha+\beta \neq \pm 1$ et $h_0 \in H$. Partant de $u_1 = u$, on construit les éléments $u_k$ de $V$ à l'aide de la relation $u_{k+1} = \frac{\beta}{\alpha} h_0 u_k + (-1)^k u_1$. En notant $m$ le plus petit entier pour lequel $h_0^m$ fixe la classe de $s$, on obtient $u_m = \frac{(-\alpha)^m - \beta^m}{\alpha^{m-1}}(\frac{-1}{\alpha+\beta} + s)e_H$ si $\frac{\beta}{\alpha} \neq -1$ et $u_m = (-1)^{m-1} m e_H$ si $\frac{\beta}{\alpha} = -1$.

Comme par hypothèse, $\alpha$ et $\beta$ sont rationnels, si $\frac{\beta}{\alpha}$ est différent de $\pm 1$, $(1-(\alpha+\beta)s)e_H$ appartient à $V$ et plus généralement $(1-(\alpha+\beta)^k s^k)e_H$ appartient à $V$. En prenant $k$ tel que $s^k \in H$, $(1-(\alpha+\beta)^k)e_H \in V$. Cela

assure que $V$ n'est pas admissible puisque $\alpha + \beta \neq \pm 1$. Il ne reste qu'à considérer les cas $\frac{\beta}{\alpha} = \pm 1$.

Si $\beta = -\alpha$, $e_H u = e_H$ et $V$ n'est pas admissible. Si $\beta = \alpha$, $u = (1 - \alpha s - \alpha h_0 s)e_H$. Le cas $\alpha = 1$ a été traité dans la proposition précédente et pour $\alpha \neq 1$, les arguments déja utilisés s'appliquent bien. On commence par remarquer que pour que $u$ soit admissible, il est nécessaire que les classes $s^{-1}H$ et $s^{-1}h_0 sH$ soient dans la même orbite sous l'action de $H$. Un calcul simple assure alors qu'il existe un entier $k$ pour lequel $v_k = (\frac{1-\alpha^k}{1-\alpha} - \frac{1-\alpha^k}{\alpha} s^{-1})e_H$ est dans $V$, ce qui assure que $V$ est non admissible dès que $\alpha$ est différent de $-1$. Le seul élément de longueur 3 qui puisse être admissible est donc un élément de la forme $(1 + s + t)e_H$.

Cette proposition s'étend à tout corps de base $k$ inclus dans le corps $\mathbb{R}$ des nombres réels.

## 3. Le cas primitif

Le groupe $H$ est désormais supposé maximal. Le module $k[G]e_H$ n'est bien sûr pas admissible. Lorsque la paire $(G, H)$ est primitive, c'est le seul sous-module non admissible avec le sous-module $k[G](e_G - e_H)$. Ce dernier sous-module est exactement l'ensemble des éléments de poids nul de $k[G]e_H$, il est engendré en tant que $k$-espace vectoriel par les $(g - 1)e_H$, $g \in G$.

**Proposition 5.** *Soit $(G, H)$ une paire primitive. Pour qu'un élément $a$ de $k[G]e_H$ et de poids non nul soit admissible, il faut et il suffit que $k[G]a$ soit différent de $k[G]e_H$, c'est à dire que l'équation $xa = e_H$ n'ait pas de solution dans $k[G]$.*

Les éléments de $G$ pour lesquels $(g - 1)e_H$ appartient à $k[G]a$ forment un sous-groupe $H'$ de $G$ qui contient $H$. Comme $H$ est maximal, si $a$ n'est pas admissible, $H' = G$ et $k[G]a$ contient $(g - 1)e_H$ pour tout $g \in G$ et par suite le sous-module $k[G](e_G - e_H)$ où $e_G = \frac{1}{|G|} \sum_{g \in G} g$. De la somme directe

$$k[G]e_H = k[G](e_G - e_H) \oplus k[G]e_G \ ,$$

on déduit l'égalité $k[G]a = k[G]e_H$ puisque $k[G]e_G = k\ e_G$ est un $k$-espace vectoriel de dimension 1 et que $k[G]a$ contient $a$ qui est de poids non nul. Ainsi si $k[G]a$ n'est pas $k[G]e_H$ tout entier, $a$ est admissible. La réciproque est évidente.

Les propositions 4 et 5 peuvent s'interpréter de la manière suivante.

**Proposition 6.** *Soit $(G, H)$ une paire primitive dont les sous-degrés sont distincts et soit $v = a_g \overline{g} + a_{g'} \overline{g'} + a_{g''} \overline{g''}$ un élément de $\mathbb{Q}[G/H]$ de poids non nul et dont les trois coefficients ne sont pas égaux. Alors $\mathbb{Q}[G]v = \mathbb{Q}[G/H]$.*

Lorsque la paire $(G, H)$ est primitive, on peut un peu améliorer la proposition 3.

**Proposition 7.** *Soient $(G, H)$ une paire primitive et $k$ un sous-corps du corps $\mathbb{C}$ des nombres complexes. S'il existe un élément admissible dans $k[G]e_H$ de la forme $a = (1 - s - t)e_H$ avec $1 \neq s \neq t \neq 1$ (mod $H$) alors, si $|G|$ est pair, au moins trois sous-degrés sont égaux et si $|G|$ est impair, au moins six sous-degrés sont égaux.*

Si $g \in G$, on note $I_g$ l'orbite de $\overline{g} \in G/H$ sous l'action à gauche de $H$. On rappelle que pour tout $g$, $|I_g| = |I_{g^{-1}}|$. Comme ci-dessus, on pose $a = (1-s-t)e_H$, $V = k[G]a$, $b = -s^{-1}a = (1-s^{-1}+s^{-1}t)e_H$, $c = -t^{-1}a = (1-t^{-1}+t^{-1}s)e_H$ et on suppose l'élément $a$ admissible. Il est clair d'après ce qui a été dit dans la démonstration de la proposition 3 que $|I_s| = |I_t|$, $|I_{s^{-1}t}| = |I_{s^{-1}}|$ avec $I_{s^{-1}t} \neq I_{s^{-1}}$ et $|I_{t^{-1}s}| = |I_{t^{-1}}|$ avec $I_{t^{-1}s} \neq I_{t^{-1}}$.

Si $I_s = I_{s^{-1}}$, il existe $h_0 \in H$ tel que $\overline{s^{-1}} = h_0\overline{s}$ et $b - h_0 a = (s^{-1}t + h_0 t)e_H$. Dans ce cas, si $\overline{s^{-1}t} = \overline{h_0 t}$, $e_H \in V$ et sinon l'admissibilité de $b - h_0 a$ induit une relation du type $x_1 + x_2 = 0$ et contredit le fait que $(G, H)$ soit primitive. Ainsi $I_s \neq I_{s^{-1}}$. D'autre part, si $I_s = I_{s^{-1}t}$, il existe $h_1 \in H$ tel que $h_1 a + b = (2 - h_1 t - s^{-1})e_H$. Un tel élément ne peut pas être admissible car il induirait ou bien une relation du type $2x_1 = 2x_2$ ou bien une relation du type $2x_1 = x_2 + x_3$ mais nous avons déja signalé qu'une telle relation est impossible lorsque les $x_i$ sont des nombres complexes dont on peut considérer le module. Ces deux arguments répétés suffisamment permettent d'affirmer que parmi les six orbites $I_s, I_{s^{-1}}, I_t, I_{t^{-1}}, I_{t^{-1}s}$ et $I_{s^{-1}t}$, les seules égalités possibles sont $I_s = I_t$ , $I_{s^{-1}} = I_{t^{-1}}$ et $I_{t^{-1}s} = I_{s^{-1}t}$ et que lorsque l'une est vraie, les trois sont vraies.

Une égalité du type $I_g = I_{g^{-1}}$ n'étant possible que lorsque $G$ est d'ordre pair, les six orbites citées ci-dessus sont bien distinctes lorsque $|G|$ est impair.

## 4. Exemples

Afin d'utiliser la proposition 7, nous supposons dans cette section que le corps $k$ est inclus dans $\mathbb{C}$. Nous avons cherché en vain à obtenir la relation $x_1 = x_2 + x_3$ pour de nombreux exemples de paires $(G, H)$ primitives ayant au moins trois sous-degrés égaux, ceux précisément qu'on ne peut pas traiter à l'aide des critères des propositions 3 et 7. On dresse dans la suite un bref bilan des situations rencontrées. On rappelle que si $a = (1 - s - t)e_H$ est un élément admissible de $k[G]e_H$, les six orbites $I_s, I_{s^{-1}}, I_t, I_{t^{-1}}, I_{t^{-1}s}$ et $I_{s^{-1}t}$ sont de même longueur et que les seules égalités possibles (et simultanées) sont $I_s = I_t$ , $I_{s^{-1}} = I_{t^{-1}}$ et $I_{t^{-1}s} = I_{s^{-1}t}$. Dans bien des cas,

*le nombre d'orbites réflexives est déterminant car lorsque les* 6 *orbites ci-dessus sont distinctes, aucune n'est réflexive et si seulement* 3 *de ces orbites sont distinctes, une et une seule est réflexive.*

Les groupes $\frac{3}{2}$-transitifs sont les groupes dont tous les sous-degrés non triviaux sont égaux. Parmi ces derniers, on distingue les $QI$-groupes (voir [2]), ceux pour lesquels dans la décomposition $1_H^G = 1 + \chi$, $\chi$ est un caractère irréductible sur le corps $\mathbb{Q}$ des rationnels. Pour un tel groupe, on a clairement $\mathbb{Q}[G](1-s-t)e_H = \mathbb{Q}[G]e_H$ et $a = (1-s-t)e_H$ n'est pas un élément admissible de $\mathbb{Q}[G]e_H$.

Le groupe $PSL(2,16)$ admet une représentation primitive en degré 120 ($H = D_{34}$), de rang 8, $\frac{3}{2}$-transitive (7 orbites non triviales de longueur 17) mais n'est pas un $QI$-groupe. Si $a = (1-s-t)e_H$ est admissible, $H = D_{34}$ entraîne que les six orbites $I_s, I_{s^{-1}}, I_t, I_{t^{-1}}, I_{t^{-1}s}$ et $I_{s^{-1}t}$ sont distintes et comme au moins deux des 7 orbites non triviales sont réflexives, ce n'est pas envisageable.

En petit degré, parmi les paires primitives qui possèdent au moins trois sous-degrés égaux, beaucoup sont des extensions décomposées de groupes abéliens du type $AH$ ( $A$ abélien, $H$ maximal qui agit sur $A$). Dans ce cas, le résultat qui suit permet de conclure. Notons qu'on trouve un résultat plus général dans [4], nous expliquons ici ce dont nous avons besoin.

**Proposition 8.** *Soit $G = AH$ une extension décomposée d'un groupe abélien $A$ par un groupe fini $H$ ($H$ agit sur $A$). Si $H$ est un sous-groupe maximal de $G$, aucun élément de la forme $(1-s-t)e_H$ avec $1 \neq s \neq t \neq 1$ ($mod\ H$) n'est admissible dans $k[G]e_H$.*

Les éléments de $k[G]e_H$ sont de la forme $\sum \lambda_a a e_H$ où $a$ appartient à $A$ et $k[G]e_H$ est $k[A]$-isomorphe à $k[A]$. Les composantes isotypiques de $k[G]e_H$ sont donc simples puisque comme $A$ est abélien, celles de $k[A]$ le sont. Ainsi, d'après la proposition 5, pour qu'un élément $\alpha = (1-s-t)e_H$ soit admissible, il faut et il suffit qu'il existe un caractère $\chi \neq 1$ appartenant à la décomposition de $1_H^G$ en caractères $k$-irréductibles tel que $\epsilon_\chi \alpha = 0$ où $\epsilon_\chi$ ($= \sum_g \chi(g^{-1})\ g$ à un facteur multiplicatif près) est l'idempotent central associé à la composante isotypique de caractère $\chi$. Notons $\epsilon_\chi e_H = \sum \mu_a a e_H$. Comme $\epsilon_\chi$ est central, $\epsilon_\chi \alpha = 0$ si et seulement si $(1-s-t)\sum \mu_a a = 0$. D'après la prop. 1, si le fixateur de $\sum \mu_a a$ est réduit à 1, $1-s-t$ est un élément admissible de $k[A]$. Mais $F = \{g \in G\ /g\epsilon_\chi e_H = \epsilon_\chi e_H\}$ est un sous-groupe de $G$ qui contient $H$, c'est donc $H$ puisque $H$ est maximal et que clairement $F \neq G$. Le fixateur de $\sum \mu_a a$ sous l'action de $A$ est donc réduit à 1 et par suite si $\alpha = (1-s-t)e_H$ est admissible dans $k[G]e_H$, $1-s-t$ est admissible dans $k[A]$ et l'ordre de $A$ est un multiple de 6, ce qui contredit le fait que $H$ soit supposé maximal.

**Théorème 2.** *Soit $(G, H)$ une paire primitive de degré $n \leq 50$. Il n'existe aucun élément admissible dans $k[G]e_H$ de la forme $a = (1 - s - t)e_H$ avec $1 \neq s \neq t \neq 1$ $(mod\ H)$ .*

D'après la proposition 7, il suffit de le vérifier pour des paires primitives qui possèdent au moins trois sous-degrés égaux. John Dixon m'a communiqué toutes ces paires primitives (déterminées à l'aide de GAP [3]) de degré $\leq 50$, elles sont données en annexe à la fin du texte. Il y en a 60 et 45 sont des extensions décomposées comme ci-dessus. Parmi les exemples restants, 11 sont des groupes diédraux. Pour un tel groupe, les orbites sont toutes réflexives et cela permet de conclure. Les 4 derniers exemples sont $PSL(2, 8)$ en degrés 28 et 36 et $PGL(2, 9)$ en degrés 36 et 45, $H$ est diédral pour chacun de ces quatre exemples. L'exemple $PSL(2, 8)$ en degré 28 peut être écarté car dans ce cas, c'est un $QI$-groupe. Pour $PGL(2, 9)$ en degré 36, $H = D_{20}$ et la situation est la suivante : On note $x$ un élément de $\mathbb{F}_9$ tel que $x^2 = 2$. En notant en ligne une matrice de $PGL(2, 9)$ $(((1, 0)(0, 1))$ pour la matrice identique), les deux matrices $a = ((1, 1)(1, x))$ et $b = ((1, 1)(1 + x, 2)$ engendrent un groupe isomorphe à $D_{20}$. Il y a trois orbites de longueur 10, celles des éléments $s_1 = ((1, 0)(0, 2))$ et $s_2 = ((1, 0)(0, x))$ sont distinctes, de longueur 10 et réflexives. Cela suffit pour écarter cet exemple. En degré 45, $H = D_{16}$ et la situation est analogue. Les deux matrices $a' = ((1, 2)(1, 1 + x))$ et $b' = ((1, x)(0, 2))$ engendrent un groupe isomorphe à $D_{16}$. Il y a trois orbites de longueur 8, celles des éléments $s'_1 = ((1, 1)(0, 2))$ et $s'_2 = ((1, 0)(0, x))$ sont distinctes, de longueur 8 et réflexives. Pour $PSL(2, 8)$ en degré 36, $H = D_{14}$ et c'est encore la même situation. Soit $y$ un élément de $\mathbb{F}_8$ tel que $y^3 = 1 + y$, c'est un générateur de $\mathbb{F}_8$ sur $\mathbb{F}_2$. Les deux matrices $c = ((1+y, 1+y)(0, y+y^2))$ et $d = ((1, 0)(1 + y, 1)$ engendrent un groupe isomorphe à $D_{14}$. Il y a trois orbites de longueur 7, celles des éléments $((0, 1)(1, 0))$ et $((1, 1 + y^2)(y, 0))$ sont distinctes, de longueur 7 et réflexives.

**Remarque.** La relation galoisienne $x_1 = x_2 + x_3$ semble difficile à obtenir dans le cas primitif. Peut-être n'est-elle même jamais vérifiée. Des relations simples et courtes existent cependant pour des paires primitives. D'après [7], la relation $x_1 = x_2 + x_3 + x_4$ est possible en degré 10 pour la paire primitive $(A_5, S_3)$ de rang 3. En rang 4, il est possible d'obtenir la relation $2x_1 = x_2 + x_3 + x_4 + x_5$ en degré 35 pour la paire primitive $(S_7, S_3 \times S_4)$ (action de $S_7$ sur les triplets $\{i, j, k\}$ de $\{1, \ldots, 7\}$) dont les sous-degrés sont 1, 4, 12 et 18. C'est l'élément $a = 2e_H - \sum_{i \in I} s_i e_H$ où $I$ désigne l'orbite de longueur 4 qui est admissible. Pour ces deux relations, les calculs sont faits dans l'algèbre $A = e_H k[G]e_H$ (un peu étudiée dans [7]) et l'élément admissible est un élément non inversible de $A$.

## Annexe. Paires primitives de degré $\leq 50$ possédant au moins trois sous-degrés égaux.

Nous donnons ci-dessous les groupes qui admettent une représentation primitive en degré $\leq 50$ et possédant au moins trois sous-degrés égaux. La codification est la suivante : $G, d, [[d_i,\ n_i]]$. L'entier $d$ désigne le degré de la représentation et $n_i$ désigne le nombre de sous-degrés égaux à $d_i$. Nous ne donnons que les sous-degrés $d_i$ pour lesquels $n_i$ est $\geq 3$. Les notations pour désigner le groupe $G$ sont classiques. Par exemple, la notation $5^2 : D(2 \times 4)$ désigne une extension décomposée du groupe abélien $C_5 \times C_5$ par le groupe diédral à 8 éléments, c'est bien sûr un produit semi-direct.

$D(2 \times 11), 11, [[2, 5]]$, $D(2 \times 13), 13, [[2, 6]]$, $13 : 3, 13, [[3, 4]]$,
$13 : 4, 13, [[4, 3]]$, $2^4 : 5, 16, [[5, 3]]$, $2^4 : D(2 \times 5), 16, [[5, 3]]$,
$D(2 \times 17), 17, [[2, 8]]$, $17 : 4, 17, [[4, 4]]$, $D(2 \times 19), 19, [[2, 9]]$,
$19 : 3, 19, [[3, 6]]$, $19 : 6, 19, [[6, 3]]$, $D(2 \times 23), 23, [[2, 11]]$,
$5^2 : 3, 25, [[3, 8]]$, $5^2 : S(3), 25, [[3, 4]]$, $5^2 : 6, 25, [[6, 4]]$,
$5^2 : Q(8), 25, [[8, 3]]$, $5^2 : D(2 \times 4), 25, [[4, 4]]$, $5^2 : 8, 25, [[8, 3]]$,
$5^2 : D(2 \times 6), 25, [[6, 4]]$, $5^2 : D(2 \times 4), 25, [[8, 3]]$, $PSL(2, 8), 28, [[9, 3]]$,
$D(2 \times 29), 29, [[2, 14]]$, $29 : 4, 29, [[4, 7]]$, $29 : 7, 29, [[7, 4]]$,
$D(2 \times 31), 31, [[2, 15]]$, $31 : 3, 31, [[3, 10]]$, $31 : 5, 31, [[5, 6]]$,
$31 : 6, 31, [[6, 5]]$, $31 : 10, 31, [[10, 3]]$, $PSL(2, 8), 36, [[7, 3]]$,
$PGL(2, 9), 36, [[10, 3]]$, $D(2 \times 37), 37, [[2, 18]]$, $37 : 3, 37, [[3, 12]]$,
$37 : 4, 37, [[4, 9]]$, $37 : 6, 37, [[6, 6]]$, $37 : 9, 37, [[9, 4]]$,
$37 : 12, 37, [[12, 3]]$, $D(2 \times 41), 41, [[2, 20]]$, $41 : 4, 41, [[4, 10]]$,
$41 : 5, 41, [[5, 8]]$, $41 : 8, 41, [[8, 5]]$, $41 : 10, 41, [[10, 4]]$,
$D(2 \times 43), 43, [[2, 21]]$, $43 : 3, 43, [[3, 14]]$, $43 : 6, 43, [[6, 7]]$,
$43 : 7, 43, [[7, 6]]$, $43 : 14, 43, [[14, 3]]$, $PGL(2, 9), 45, [[8, 3]]$,
$D(2 \times 47), 47, [[2, 23]]$, $7^2 : 4, 49, [[4, 12]]$, $7^2 : S(3), 49, [[3, 6], [6, 5]]$,
$7^2 : D(2 \times 4), 49, [[4, 6], [8, 3]]$, $7^2 : Q(8), 49, [[8, 6]]$, $7^2 : 8, 49, [[8, 6]]$,
$7^2 : Q(12), 49, [[12, 4]]$, $7^2 : D(2 \times 6), 49, [[6, 6]]$, $7^2 : 12, 49, [[12, 4]]$,
$7^2 : D(2 \times 8), 49, [[8, 6]]$, $7^2 : 16, 49, [[16, 3]]$, $7^2 : Q(16), 49, [[16, 3]]$,
$7^2 : 3 : D(2 \times 4), 49, [[12, 4]]$, $7^2 : Q(8) : 3, 49, [[8, 3]]$, $7^2 : Q(16) : 2, 49, [[16, 3]]$ .

## Bibliographie

[1] J. D. DIXON, *Polynomials with relations between their roots*. Acta Arithmetica **82.3** (1997), 293–302.

[2] J. D. DIXON, *Permutation representations and rationnal irreducibility*. Bull. Austral. Math. Soc. **71** (2005), 493–503.

[3] THE GAP GROUP, *GAP–Groups, Algorithms, and Programming*. Version 4.4.11 (2008) (http ://www.gap-system.org).

[4] K. GIRSTMAIR, *Linear relations between roots of polynomials*. Acta Arithmetica **89.1** (1999), 53–96.

[5] K. GIRSTMAIR, *The Galois relation $x_1 = x_2 + x_3$ and Fermat over finite fields*. Acta Arithmetica **124.4** (2006), 357–370.

[6] K. GIRSTMAIR, *The Galois relation $x_1 = x_2 + x_3$ for finite simple groups*. Acta Arithmetica **127.3** (2007), 301–303.

[7] F. LALANDE, *Relations linéaires entre les racines d'un polynôme et anneaux de Schur*. Ann. Sci. Math. Québec **27.2** (2003), 169–175.

[8] F. LALANDE, *La relation linéaire $a = b + c + \ldots + t$ entre les racines d'un polynôme*. J. Théorie des Nombres de Bordeaux **19** (2007), 473–484.

## APPENDICE

par Joseph OESTERLÉ

Soient $G$ un groupe fini d'ordre $n$ et $k$ un corps commutatif dont la caractéristique est 0, ou un nombre premier qui ne divise pas $n$. Nous dirons qu'un élément $a$ de $k[G]$ est *admissible* si $k[G]a$ ne contient aucun élément de la forme $g - e$, avec $g \in G$ distinct de l'élément neutre $e$.

**Remarque.** Soient $k'$ un sous-corps de $k$ et $G'$ un sous-groupe de $G$ tels que $a \in k'[G']$. Alors $a$ est un élément admissible de $k'[G']$ si et seulement si c'est un élément admissible de $k[G]$.

**Proposition.** *Soit $L$ une extension galoisienne de $k$, de groupe de Galois $G$. Pour qu'un élément $a \in k[G]$ soit admissible, il faut et il suffit qu'il existe un élément primitif $x$ de $L$ tel que $ax = 0$.*

Supposons qu'il existe un élément primitif $x$ de $L$ tel que $ax = 0$. Pour tout $g \in G$ distinct de $e$, on a $g(x) \neq x$ et donc $g - e \notin k[G]a$. Par suite $a$ est admissible.

Supposons inversement $a$ admissible. Notons $V$ le $k[G]$-module à gauche $k[G]/k[G]a$ et $v$ l'image canonique de $e$ dans $V$. On a $av = 0$ et $gv \neq v$ pour tout $g \in G$ distinct de $e$. Comme le $k[G]$-module à gauche $k[G]$ est semi-simple, son sous-module $k[G]a$ possède un supplémentaire. Donc $V$ est isomorphe à un sous-$k[G]$-module de $k[G]$, et d'après le théorème de la base normale à un sous-$k[G]$-module de $L$. Par suite, il existe un élément $x$ de $L$ tel que $ax = 0$ et $gx \neq x$ pour tout $g \in G$ distinct de $e$ ; c'est un élément primitif de $L$ annulé par $a$.

**Théorème.** *Supposons que l'ordre de $G$ soit multiple de 6. Soient $s$ un élément de $G$ d'ordre 2 et $t$ un élément de $G$ d'ordre 3. Alors $a = e - st - st^2$ est un élément admissible de $k[G]$.*

Nous aurons besoin au cours de la démonstration du lemme suivant :

**Lemme 1.** *Soit $F$ un espace vectoriel sur $k$ de dimension finie $d$ et soit $(e_i)_{i \in I}$ une base de $F$. Soient $r$ un entier $\geq 1$ et $S$ une partie de $F$ telle que :*

*a) chaque élément de $S$ a au plus $r$ coordonnées non nulles dans la base $(e_i)_{i \in I}$ ;*

*b) pour tout $i \in I$, il existe un élément de $S$ dont la coordonnée d'indice $i$ est $\neq 0$.*

*Le sous-espace vectoriel de $F$ engendré par $S$ est alors de dimension $\geq \frac{d}{r}$.*

Soit en effet $S'$ une partie libre maximale de $S$ et soit $m$ son cardinal. Si $m < \frac{d}{r}$, il existe d'après $a$) un indice $i \in I$ tel que les coordonnées d'indice $i$ de tous les éléments de $S'$ soient nulles et il existe d'après $b$) un élément

$s \in S$ dont la coordonnée d'indice $i$ est non nulle. Mais alors $S' \cup \{s\}$ est une partie libre de $S$, ce qui contredit la maximalité de $S'$. On a donc $m \geq \frac{d}{r}$, d'où le lemme.

Démontrons maintenant le théorème. Il résulte de la relation $a = (e+s) - s(e+t+t^2)$ que $k[G]a$ est contenu dans $k[G](e+s) + k[G](e+t+t^2)$. L'ensemble des éléments $h \in G$ tels que $h - e \in k[G](e+s) + k[G](e+t+t^2)$ est un sous-groupe de $G$ puisque l'on a $hh' - e = h(h'-e) + h - e$. Il suffit de démontrer que ce sous-groupe est réduit à l'élément neutre, ce qui résulte des deux lemmes suivants :

**Lemme 2.** *La dimension de* $k[G]/(k[G](e+s) + k[G](e+t+t^2))$ *est au moins* $\frac{n}{6} + 1$.

En effet la dimension de $k[G]$ est $n$, celle de $k[G](e+s)$ est $\frac{n}{2}$, celle de $k[G](e+t+t^2)$ est $\frac{n}{3}$ et celle de $k[G](e+s) \cap k[G](e+t+t^2)$ est $\geq 1$ puisque $\sum_{g \in G} g$ appartient à cette intersection.

**Lemme 3.** *Soit* $H$ *un sous-groupe de* $G$ *non réduit à l'élément neutre. La dimension de* $E = k[G]/(k[G](e+s) + k[G](e+t+t^2) + \sum_{h \in H} k[G](h-e))$ *est au plus* $\frac{n}{6}$.

Comme $shs - e = sh(e+s) - s(h-e) - (e+s)$, on peut remplacer $H$ par le sous-groupe engendré par $H$ et $sHs$ sans changer $E$, c'est à dire supposer que $H$ est normalisé par $s$.

L'espace vectoriel $E$ est isomorphe à $k[G/H]/(k[G](\overline{e}+\overline{s}) + k[G](\overline{e}+\overline{t}+\overline{t^2}))$, où $\overline{g}$ désigne la classe à gauche $gH$ de $g$ modulo $H$. Notons $m$ l'ordre de $H$. La dimension de $k[G/H]$ est $\frac{n}{m}$. Il résulte du lemme 1, appliqué à l'espace vectoriel $k[G/H]$ muni de sa base canonique et à sa partie $S$ formée des éléments $\overline{g} + \overline{gs}$, où $g \in G$, que la dimension du sous-espace vectoriel $k[G](\overline{e}+\overline{s})$ de $k[G/H]$ est $\geq \frac{n}{2m}$. On a donc $\dim(E) \leq \frac{n}{2m}$, ce qui implique le lemme 3 lorsque $m \geq 3$.

Il reste à considérer le cas où $H$ est un groupe d'ordre 2 normalisé par $s$, *i.e.* de la forme $\{e, \sigma\}$, avec $s\sigma = \sigma s$. Si $\sigma = s$, on a $\overline{e} + \overline{s} = 2\overline{e}$, donc $E = 0$ et le lemme s'en suit. Supposons donc $\sigma \neq s$. Alors $H' = \{e, s, \sigma, s\sigma\}$ est un sous-groupe d'ordre 4 de $G$. Choisissons un système de représentants $R$ dans $G$ des classes à gauche de $G/H'$. Les images $[r]$ des éléments $r$ de $R$ dans $F = k[G]/(k[G](e+s) + k[G](\sigma - e))$ forment une base de l'espace vectoriel $F$, qui est de dimension $\frac{n}{4}$. Notons $S$ l'ensemble des images dans $F$ des éléments de la forme $g + gt + gt^2$, où $g \in G$. Chacun de ces éléments a au plus 3 coordonnées non nulles dans la base $([r])_{r \in R}$. De plus, pour tout $r \in R$, l'élément $r + rt + rt^2$ a une coordonnée d'indice $[r]$ égale à 1, puisque $rt$ et $rt^2$ n'appartiennent pas à $rH'$. Il s'en suit d'après le lemme 1 que le

sous-espace vectoriel de $F$ engendré par $S$ est de dimension $\geq \frac{n}{12}$ et donc que l'on a $\dim(E) \leq \frac{n}{4} - \frac{n}{12} = \frac{n}{6}$.

Franck Lalande
38, grande rue
89140 Gisy les nobles, France
*E-mail*: lalande072@orange.fr